18. Active Directory - Fundamentals

🧠 1. What is Active Directory (AD)?

Active Directory (AD) is a **directory service** developed by Microsoft for **Windows domain networks**.

🔹 Key Functions:

- Centralized **authentication and authorization**.
- Manages **users, computers, printers, and other resources**.
- Organizes network objects into **hierarchical structures** like **domains**, **trees**, and **forests**.

🔹 Use Case:

- Enterprises use AD to enforce **Group Policies**, manage **user accounts**, and provide **Single Sign-On (SSO)** capabilities across systems.

> 📁 AD stores data using a **hierarchical structure** and relies on **LDAP**, **Kerberos**, and **DNS** for its operations.

🔐 2. What is Authentication?

Authentication is the process of **verifying a user's identity**.

🔹 Examples:

- Username + password
- Smart cards or biometrics
- OTP (One-Time Passwords)

🔹 Common Protocols:

- **Kerberos** (used in AD)
- **NTLM**
- **OAuth / SAML** (for web apps)

> 🧠 Think: *“Who are you?”*

🎫 3. What is Authorization?

Authorization is the process of **granting or denying access to resources after authentication**.

🔹 Examples:

- A user logs in (authenticated) but can only access files they have permissions for (authorized).
- Role-Based Access Control (RBAC)

> 🧠 Think: *“What are you allowed to do?”*

🖥️ 4. What is a Domain Controller (DC)?

A **Domain Controller (DC)** is a **server that manages security and access** within a domain in Active Directory.

🔹 Key Roles:

- Handles **authentication requests** (e.g., logins).
- Applies **Group Policies**.
- Manages **user and device accounts**.

> ✅ AD environments typically have **Primary DCs** and **Backup DCs** for redundancy.

🌐 5. What is a Domain (in AD)?

A **Domain** is a **logical grouping of resources** (users, computers, devices) that share the same **AD database** and policies.

🔹 Naming:

- Domains are often named like DNS entries (e.g., `corp.example.com`).

🔹 Purpose:

- Define **trust boundaries**.
- Provide **centralized management** for resources.

> 🧱 Multiple domains can exist in a **forest**, connected via **trusts**.

📚 6. What is LDAP (Lightweight Directory Access Protocol)?

LDAP is a **protocol used to access and manage directory services** like Active Directory.

🔹 Functions:

- Query user accounts
- Authenticate users
- Manage permissions and directory objects

🔹 Example Query:

```
ldapsearch -x -h ldap.example.com -b "dc=example,dc=com"
```

🔹 **Ports:**

- **389** (LDAP)
- **636** (LDAPS - secure)

> 🛡️ LDAP is **crucial** in penetration testing and red teaming when enumerating users or querying Active Directory.

🧩 Summary Table

Term	Description
Active Directory	Microsoft directory service to manage users/resources
Authentication	Verifies **who** the user is
Authorization	Determines **what** the user can access
Domain Controller	Server that handles authentication and applies policies
Domain	Logical grouping of resources under a single AD structure
LDAP	Protocol used to interact with directory services
